UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,459	12/29/2003	Bing Wang	059643.00747	7057

32294 7590 11/24/2009

SQUIRE, SANDERS & DEMPSEY L.L.P.
8000 TOWERS CRESCENT DRIVE
14TH FLOOR
VIENNA, VA 22182-6212

EXAMINER	
MAI, KEVIN S	

ART UNIT	PAPER NUMBER
2456	

MAIL DATE	DELIVERY MODE
11/24/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/748,459
Filing Date: December 29, 2003
Appellant(s): WANG, BING

Bing Wang
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed August 24, 2009 appealing from the Office action mailed December 8, 2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 1, 2, 4-9, 11-16 and 18-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo").

2. **As to Claim 1,** Araujo discloses **a method, comprising:**

receiving a request from a client device for access to an application associated with a network device (Paragraph [0084] of Araujo discloses the user can then click on any of these icons (request), which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application)**;**

establishing a session between a unified session manager and a management server associated with the application (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose**, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device;**

modifying the request at the unified session manager (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**;**

forwarding, by the unified session manager, the modified request to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**;**

receiving a response at the unified session manager from the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**;**

modifying the response at the unified session manager (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**; and**

forwarding, by the unified session manager, the modified response to the client device (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**.**

Araujo does not explicitly disclose, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

3. **As to Claim 2,** Araujo discloses the invention as claimed as described in claim 1**, wherein the request is authenticated by the unified session manager** (Paragraph [0121] of Araujo discloses the SEP maintains lists of authorized user names and passwords, and, based on login information supplied by a user then seeking remote access, determining whether that user is permitted to access the applications)**.**

4. **As to Claim 4,** Araujo discloses the invention as claimed as described in claim 1**, wherein modifying the request further comprises translating a graphical user interface message and, wherein modifying the response further comprises translating another**

graphical user interface message (Paragraph [0120] of Araujo discloses receiving user mouse clicks and keystrokes from the user browser in AIP form and translating them to RDP. Where clicks are seen include clicking on icons to cause applications to open and thus seen to be GUI messages (paragraph [0084]). Then paragraph [0120] discloses receiving graphical output displays from the client application in RDP and translating them to AIP).

5. **As to Claim 5,** Araujo discloses the invention as claimed as described in claim 4, **wherein at least one of the graphical user interface message and the other graphical user interface message is translated into a unified format (**Paragraph [0120] of Araujo discloses the requests being converted from AIP form to RDP and then the responses being converted from RDP form to AIP. These are both seen to be the GUI messages being translated into unified formats).

6. **As to Claim 6,** Araujo discloses the invention as claimed as described in claim 1, **wherein modifying the request further comprises modifying a network address before forwarding the modified request, and wherein modifying the response further comprises modifying another network address before forwarding the modified response** (Paragraph [0092] of Araujo discloses the SEP can intercept incoming network messages and perform required protocol conversion and IP address translation on each message and provide the opposite functionality in a reverse direction for outgoing messages. This is further clarified in paragraph [0097]).

7. **As to Claim 7,** Araujo discloses the invention as claimed as described in claim 1**, wherein modifying the response further comprises enabling a download of a file from the unified session manager** (Paragraph [0084] of Araujo discloses after a user clicks an icon to launch an application the SEP will launch the associated office application and generate an HTML file for graphical display produced by that application and then download the HTML file to the users browser)**.**

8. **As to Claim 8,** Araujo discloses **an apparatus, comprising:**
a transceiver configured to receive a request from a client for access to an application on the network device and to forward a response to the request (Figure 2 of Araujo discloses a set of Ethernet ports on the SEP. Paragraph [0120] discloses the SEP taking in requests from the client and sending responses back to the client)**; and**
a processor (Figure 2 and paragraph [0091] of Araujo disclose the SEP having a microprocessor)**, coupled to the transceiver, that is configured to**
establish a session on behalf of the client between the unified session manager and a management server associated with the application (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose**, wherein the session is established with the management server by the processor which is further configured to authenticate the unified session manager to the management server, and wherein the authentication is virtually transparent to the client device,**

modify the request (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**,**

forward the modified request to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**,**

receive the response on behalf of the client from the management server associated with the application (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**,**

modify the response (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**, and**

forward the modified response from the management server to the transceiver (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120]

discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user).

Araujo does not explicitly disclose wherein the session is established with the management server by the processor which is further configured to authenticate the unified session manager to the management server, and wherein the authentication is virtually transparent to the client device.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

9. **As to Claim 9,** Araujo discloses the invention as claimed as described in claim 8, **wherein the processor is further configured to authenticate the request** (Paragraph [0121] of Araujo discloses the SEP maintains lists of authorized user names and passwords, and, based on login information supplied by a user then seeking remote access, determining whether that user is permitted to access the applications).

10. **As to Claim 11,** Araujo discloses the invention as claimed as described in claim 10**, wherein the authentication to the management server further comprises sending at least one of a password, a certificate, and an encryption key** (Paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. SSL is known to utilize certificates and encryption keys in its authentication process and thus it is seen that the authentication between the SEP and the Application server comprises those things)**.**

11. **As to Claim 12,** Araujo discloses the invention as claimed as described in claim 8**, wherein the processor is further configured to modify at least one of the request and the response by translating at least one graphical user interface message** (Paragraph [0120] of Araujo discloses receiving user mouse clicks and keystrokes from the user browser in AIP form and translating them to RDP. Where clicks are seen include clicking on icons to cause applications to open and thus seen to be GUI messages (paragraph [0084]). Then paragraph [0120] discloses receiving graphical output displays from the client application in RDP and translating them to AIP)**.**

12. **As to Claim 13,** Araujo discloses the invention as claimed as described in claim 8**, the processor is further configured to**
establish another session on behalf of the client with another application (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session). As to it being another session Paragraph [0084] discloses

the user can readily move between one remote office application to the next by simply clicking on the associated icon, this further applies to the remaining limitations);

modify another request (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

forward the other modified request to the application (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

receive another response on behalf of the client from the application (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user);

modify the other response (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user); **and**

forward the other modified response to the transceiver (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator

to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user).

13. **As to Claim 14,** Araujo discloses the invention as claimed as described in claim 8, **wherein the processor is further configured to enable a plurality of clients to access virtually simultaneously a plurality of applications on the network device** (Paragraph [0077] of Araujo discloses the SEP can simultaneously accommodate multiple clients. Then paragraph [0084] discloses the SEP allowing the user to readily move between one remote office application to another).

14. **As to Claim 15,** Araujo discloses **a method comprising:**

establishing a session between a unified session manager and at least one of a plurality of the management servers, wherein the unified session manager is enabled to operate on behalf of at least one of a plurality of clients (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session). As to there being a plurality of management servers, paragraph [0084] discloses the user can readily move between office applications by clicking on associated icons, thus there are a plurality of management servers. Then as to there being a plurality of clients, paragraph [0077] of Araujo discloses the SEP can simultaneously accommodate multiple clients). Araujo does not explicitly disclose**, and wherein establishing the session with the at**

least one of the management servers further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the clients; and

modifying each message from the at least one of the plurality of clients destined for an application associated with the at least one of the plurality of the management servers, wherein the modification is virtually transparent to the client and to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application).

Araujo does not explicitly disclose, and wherein establishing the session with the at least one of the management servers further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the clients.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

15. **As to Claim 16,** Araujo discloses the invention as claimed as described in claim 15, **wherein the unified session manager is enabled to operate on behalf of each of the plurality of clients seeking access to the at least one of the plurality of management servers** (Paragraph [0077] of Araujo discloses the SEP can simultaneously accommodate multiple clients. Then paragraph [0084] discloses the SEP allowing the user to readily move between one remote office application to another).

16. **As to Claim 18,** Araujo discloses the invention as claimed as described in claim 15, **wherein modifying each message between the at least one of the plurality of the clients and the at least one of the plurality of the management servers further comprises at least one of wrapping a Java applet** (Figure 11 of Araujo discloses using a Java Applet (1180)), **and translating a uniform resource locator** (Paragraph [0036] of Araujo discloses the SEP taking in input in the form of URI/URL selection).

17. **As to Claim 19,** Araujo discloses **a method, comprising:**
retrieving a set of menu entries including at least one menu entry that is associated with a remote application (Figure 18 of Araujo discloses displaying to the user the applications available to them);
displaying a selection menu on a display comprising the set of menu entries (Figure 18 of Araujo discloses displaying to the user the applications available to them);

retrieving a menu entry selection signal, wherein the menu entry selection signal is modified by a unified session manager (Paragraph [0084] of Araujo discloses the user can click on any of the application icons to cause the SEP to launch the associated office application. Then paragraph [0120] discloses how mouse clicks are sent in AIP form and converted to RDP by the SEP);

forwarding the modified menu entry selection signal to a management server associated with the remote application (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

receiving another signal indicative of a response from the management server, wherein the other signal is modified by the unified session manager (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user);

establishing a session between the unified session manager and the management server associated with the application (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose**, wherein establishing the session with the management server**

further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to a client device; and displaying the other modified signal at the display (Paragraph [0120] of Araujo discloses the screen shots from the application are sent to the user to be rendered by the user's browser)**.**

Araujo does not explicitly disclose wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to a client device.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

18. **As to Claim 20,** Araujo discloses the invention as claimed as described in claim 19**, wherein the menu entry selection signal comprises, a request for authentication, and a request for a program download** (Paragraph [0084] of Araujo discloses how a user must first login to be authorized to do anything, wherein the act of logging in is seen as having been authenticated. Then paragraph [0154] discloses when a user clicks on the "My Apps" tab an

HTML page that contains a Java applet is downloaded to the browser, wherein the java applet is seen to be the program).

19. **As to Claim 21,** Araujo discloses the invention as claimed as described in claim 19, **wherein modifying the menu entry selection signal further comprises translating a graphical user interface message** (Paragraph [0120] of Araujo discloses receiving user mouse clicks and keystrokes from the user browser in AIP form and translating them to RDP. Where clicks are seen include clicking on icons to cause applications to open and thus seen to be GUI messages (paragraph [0084])), **altering a network address** (Paragraph [0092] of Araujo discloses the SEP can intercept incoming network messages and perform required protocol conversion and IP address translation on each message and provide the opposite functionality in a reverse direction for outgoing messages. This is further clarified in paragraph [0097]), **and attaching additional information to the signal** (Paragraph [0110] of Araujo discloses performing SSL operations on the data. This is seen to be adding additional information to the signal).

20. **As to Claim 22,** Araujo discloses the invention as claimed as described in claim 19, **wherein modifying the other signal, indicative of a response from the management server, further comprises translating a graphical user interface message** (Paragraph [0120] or Araujo discloses receiving graphical output displays from the client application in RDP and translating them to AIP), **altering a network address** (Paragraph [0092] of Araujo discloses the SEP can intercept incoming network messages and perform required protocol conversion and IP

address translation on each message and provide the opposite functionality in a reverse direction for outgoing messages. This is further clarified in paragraph [0097])**, and attaching additional information to the signal** (Paragraph [0111] of Araujo discloses using the Open SSL module to provide appropriate security functions to the response. This is seen to be adding additional information to the signal)**.**

21. **As to Claim 23,** Araujo discloses **an apparatus, comprising:**

a means for establishing a session with a management server associated with an application on behalf of a remote client (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose**, wherein establishing the session with the management server further comprises authenticating means for authenticating the unified session manager to the management server, wherein the authenticating means is virtually transparent to the client;**

a means for modifying the request (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**;**

a first forwarding component configured to forward the modified request to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional

communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application);

a means for receiving a response from the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user);

a means for modifying the response (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user); **and**

a second forwarding component configured to forward the modified response to the remote client (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user).

Araujo does not explicitly disclose, wherein establishing the session with the management server further comprises authenticating means for authenticating the unified session manager to the management server, wherein the authenticating means is virtually transparent to the client.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

22. **As to Claim 24,** Araujo discloses **an apparatus, comprising:**

an establisher configured to establish a session with a management server associated with an application on behalf of a remote client (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose**, wherein the session is established with the management server by an authentication with a unified session manager to the management server, and wherein the authentication is virtually transparent to the remote client;**

a modifier configured to modify a request (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**;**

a request forwarder configured to forward the modified request to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**;**

a receiver configured to receive a response from the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**;**

a modifier configured to modify the response (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**; and**

a response forwarder configured to forward the modified response to the remote client (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**.**

Araujo does not explicitly disclose wherein the session is established with the management server by an authentication with a unified session manager to the management server, and wherein the authentication is virtually transparent to the remote client.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

23. **As to Claim 25,** Araujo discloses **a computer program embodied on a computer readable medium, said computer program configured to control a processor to perform: receiving a request from a client device for access to an application associated with a network device** (Paragraph [0084] of Araujo discloses the user can then click on any of these icons (request), which, once communicated back to SEP (service enablement platform), will cause the SEP to launch the associated office application)**;**
establishing a session between a unified session manager and a management server associated with the application (Paragraph [0084] of Araujo discloses the user can then click on any of these icons, which, once communicated back to SEP (service enablement platform),

will cause the SEP to launch the associated office application (establishing a session)). Araujo does not explicitly disclose**, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device;**

modifying the request at the unified session manager (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**;**

forwarding, by the unified session manager, the modified request to the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP receiving input via AIP form from the user and converting it to RDP to send to the client application)**;**

receiving a response at the unified session manager from the management server (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**;**

modifying the response at the unified session manager (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining

graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**; and**

forwarding, by the unified session manager, the modified response to the client device (Paragraph [0086] of Araujo discloses the SEP acts as a bridge between the user and the office applications and as a protocol translator to enable bi-directional communication. Then paragraph [0120] discloses the SEP obtaining graphical output displays in RDP form from the client application and converts them to AIP messages to send back to the user)**.**

Araujo does not explicitly disclose, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device.

However, paragraph [0109] of Araujo discloses that all information transfer for the Virtual Office is protected by SSL. The SEP and the Application servers communicate using SSL and using SSL is known to inherently include an authentication step. Thus it is seen that the SEP and the Applications servers authenticate themselves utilizing the SSL protocol. This is seen to be transparent to the client device since the client device has no participation in it. Thus it would have been obvious to a person having ordinary skill in the art that because Araujo discloses communication using SSL between the SEP and the application servers, that the SEP and application servers would authenticate each other, wherein the authentication is transparent to the client.

(10) Response to Argument

The examiner summarizes the various points raised by the appellant and addresses replies individually.

As per appellant's argument that:

(1) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that the Office Action's analysis is incorrect and although Araujo does state in paragraph [0109] that for the Netilla virtual office, all information transfer is protected by SSL, it is made clear by Araujo that SSL is only utilized for communications to and from the remote client via the WAN and is not in fact used for communications between the SEP and the LAN including the application servers.

In response to argument (1), examiner asserts that the examiner's original analysis is correct. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN.

(2) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"),

appellant argues that according to paragraph [0109] of Araujo it is clear that the incoming packet is authenticated and decrypted prior to extraction of the content of the packet extraction and subsequent translation by the virtual office software. The HTTP request is thus extracted, translated and sent directed to the office application without passing back via the open SSL module for encryption prior to being sent to the application server. As such, there is no SSL encryption used for communications between the SEP and the application server.

In response to argument (2), examiner asserts that just because the information is not sent back through the open SSL module does not mean that no SSL encryption is used for communications between the SEP and the application server. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software 400 has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software 400 to that office application accessible through the LAN via path 402. Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN. Thus since the virtual office software is capable of performing SSL operations it is seen that the requirement of having to go through the open SSL module is not valid.

(3) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that their interpretation is confirmed as being correct with further reference in paragraph [0111] of Araujo, which describes the processing of packets received by the SEP from

the LAN. These packets are received along data path 402 shown in Figure 3b. The path flows through to the virtual office software 400 without pass through web server 350 and without calling on the open SSL module 340. The virtual office software 400 generates an appropriate HTML page and only then passes the HTML page to web server 350. The web server 350 then calls on the serves of the open SSL module 340 to encrypt the HTML page and sent it to the remote client via the WAN.

In response to argument (3), examiner asserts that while the Figure 3b may show the paths as such, the assumption that not passing through the web server indicates the system does not use SSL between the SEP and the LAN is not valid. As pointed out by the applicant Figure 3b does show a path (402) from the WAN going to virtual office software without going through the web server. However this does not mean no SSL operations were performed during this path. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software 400 has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software 400 to that office application accessible through the LAN via path 402. Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN. Thus it is seen that the assumption that not passing through the web server indicates the system does not use SSL between the SEP and the LAN is not valid since the virtual office software is capable of performing SSL operations.

(4) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that in light of their previous arguments it is clear that the mention of "all information transfer is protected by SSL" in paragraph [0109] of Araujo actually relates to all information transferred between the remote client and the SEP via the WAN. No authentication and encryption protocols are utilized between the SEP and the LAN.

In response to argument (4), examiner asserts that the examiner's original analysis is correct. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN.

(5) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that the reason no encryption protocol is required in Araujo between the SEP and the LAN is that the SEP is authenticated during an initial installation process with the centralized administrative website.

In response to argument (5), examiner asserts that this does not indicate that no SSL communication occurs between the SEP and LAN. Paragraph [0109] of Araujo states that for

the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN.

(6) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that it is clear that there is no disclosure or suggestion in Araujo that establishing a session between the SEP and management server associated with an application comprises authenticating the SEP with the management server associated with the application. Rather, the SEP in Araujo is authenticated with a centralized administrative website during installation and subsequent communications between a remote client and the SEP via the WAN utilize SSL.

In response to argument (6), examiner asserts that this is not clear because Araujo does suggest such a feature. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402).

Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN.

(7) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that the arrangement describe in Araujo is adapted for use in small to medium sized organizations and specifically for remotely accessing an internal office network remotely by employees. No authentication or encryption protocols are required between the SEP and the LAN as these are all located within the local office network environment. Appellant states that the present invention may have applications and management servers associated therewith may not be provided in a safe office intranet environment. Accordingly, the arrangement of Araujo is not appropriate for the user intended for the present invention. Appellant further states that an authentication process is not required in Araujo.

In response to argument (7), examiner asserts that most of those points are not relevant to the claim language and are not necessarily supported by Araujo. Araujo does not state that no authentication or encryption protocols are required between the SEP and the LAN. Furthermore it would appear otherwise, paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402).

Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN.

(8) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that the Advisory Action argued that "this alone is not enough to determine that SSL would not be used between the SEP and the LAN". Appellant respectfully notes that this burden is on the Office Action to positively demonstrate disclosure.

In response to argument (8), examiner asserts that the Office Action has done so. The Office Action initially stated that paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. This was deemed to be indication enough since it indicated that all information transfer is protected using SSL. However to further support examiners interpretation, paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN.

(9) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that for claim 1 in view of the arguments set forth above, it is respectfully

submitted that "wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device" is neither disclosed nor suggested in Araujo.

In response to argument (9), examiner asserts that Araujo does at least suggest this feature. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN. Thus as recited in the Office Action, since the connection utilizes SSL, it is seen that it would be obvious for the components to perform authentication.

(10) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 2 depends from and further limits claim 1. Thus, claim 2 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 1.

In response to argument (10), examiner asserts that Araujo discloses the features of claim 1 and recites the same rational as that used for argument (9). Appellant has indicated that claim 2 should be allowed because it further limits claim 1, however appellant has not provided further

arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 2.

(11) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 4 depends from and further limits claim 1. Thus, claim 4 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 1.

In response to argument (11), examiner asserts that Araujo discloses the features of claim 1 and recites the same rational as that used for argument (9). Appellant has indicated that claim 4 should be allowed because it further limits claim 1, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 4.

(12) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 5 depends from and further limits claim 4. Thus, claim 5 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 4.

In response to argument (12), examiner asserts that Araujo discloses the features of claim 4 and recites the same rational as that used for argument (11). Appellant has indicated that claim 5 should be allowed because it further limits claim 4, however appellant has not provided further

arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 5.

(13) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 6 depends from and further limits claim 1. Thus, claim 6 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 1.

In response to argument (13), examiner asserts that Araujo discloses the features of claim 1 and recites the same rational as that used for argument (9). Appellant has indicated that claim 6 should be allowed because it further limits claim 1, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 6.

(14) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 7 depends from and further limits claim 1. Thus, claim 7 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 1.

In response to argument (14), examiner asserts that Araujo discloses the features of claim 1 and recites the same rational as that used for argument (9). Appellant has indicated that claim 7 should be allowed because it further limits claim 1, however appellant has not provided further

arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 7.

(15) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that for claim 8 in view of the arguments set forth above, it is respectfully submitted that "establish a session on behalf of the client between the unified session manager and a management server associated with the application, wherein the session is established with the management server by the processor which is further configured to authenticate the unified session manager to the management server, and wherein the authentication is virtually transparent to the client device" is neither disclosed nor suggested in Araujo.

In response to argument (15), examiner asserts that Araujo does at least suggest this feature. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN. Thus as recited in the Office Action, since the connection utilizes SSL, it is seen that it would be obvious for the components to perform authentication.

(16) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 9 depends from and further limits claim 8. Thus, claim 9 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 8.

In response to argument (16), examiner asserts that Araujo discloses the features of claim 8 and recites the same rational as that used for argument (15). Appellant has indicated that claim 9 should be allowed because it further limits claim 8, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 9.

(17) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 11 depends from and further limits claim 8. Thus, claim 11 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 8.

In response to argument (17), examiner asserts that Araujo discloses the features of claim 8 and recites the same rational as that used for argument (15). Appellant has indicated that claim 11 should be allowed because it further limits claim 8, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 11.

(18) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 12 depends from and further limits claim 8. Thus, claim 12 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 8.

In response to argument (18), examiner asserts that Araujo discloses the features of claim 8 and recites the same rational as that used for argument (15). Appellant has indicated that claim 12 should be allowed because it further limits claim 8, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 12.

(19) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 13 depends from and further limits claim 8. Thus, claim 13 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 8.

In response to argument (19), examiner asserts that Araujo discloses the features of claim 8 and recites the same rational as that used for argument (15). Appellant has indicated that claim 13 should be allowed because it further limits claim 8, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 13.

(20) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 14 depends from and further limits claim 8. Thus, claim 14 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 8.

In response to argument (20), examiner asserts that Araujo discloses the features of claim 8 and recites the same rational as that used for argument (15). Appellant has indicated that claim 14 should be allowed because it further limits claim 8, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 14.

(21) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that for claim 15 in view of the arguments set forth above, it is respectfully submitted that "establishing a session between a unified session manager and at least one of a plurality of the management servers, wherein the unified session manager is enabled to operate on behalf of at least one of a plurality of clients, and wherein establishing the session with the at least one of the management servers further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the clients" is neither disclosed nor suggested in Araujo.

In response to argument (21), examiner asserts that Araujo does at least suggest this feature. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information

transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN. Thus as recited in the Office Action, since the connection utilizes SSL, it is seen that it would be obvious for the components to perform authentication.

(22) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 16 depends from and further limits claim 15. Thus, claim 16 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 15.

In response to argument (22), examiner asserts that Araujo discloses the features of claim 15 and recites the same rational as that used for argument (21). Appellant has indicated that claim 16 should be allowed because it further limits claim 15, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 16.

(23) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"),

appellant argues that claim 18 depends from and further limits claim 15. Thus, claim 18 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 15.

In response to argument (23), examiner asserts that Araujo discloses the features of claim 15 and recites the same rational as that used for argument (21). Appellant has indicated that claim 18 should be allowed because it further limits claim 15, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 18.

(24) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that for claim 19 in view of the arguments set forth above, it is respectfully submitted that "establishing a session between the unified session manager and the management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to a client device" is neither disclosed nor suggested in Araujo.

In response to argument (24), examiner asserts that Araujo does at least suggest this feature. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly

from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN. Thus as recited in the Office Action, since the connection utilizes SSL, it is seen that it would be obvious for the components to perform authentication.

(25) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 20 depends from and further limits claim 19. Thus, claim 20 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 19.

In response to argument (25), examiner asserts that Araujo discloses the features of claim 19 and recites the same rational as that used for argument (24). Appellant has indicated that claim 20 should be allowed because it further limits claim 19, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 20.

(26) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 21 depends from and further limits claim 19. Thus, claim 21 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 19.

In response to argument (26), examiner asserts that Araujo discloses the features of claim 19 and recites the same rational as that used for argument (24). Appellant has indicated that claim 21 should be allowed because it further limits claim 19, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 21.

(27) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that claim 22 depends from and further limits claim 19. Thus, claim 22 should be allowed over Araujo for at least the reasons stated above, as well as because it further limits claim 19.

In response to argument (27), examiner asserts that Araujo discloses the features of claim 19 and recites the same rational as that used for argument (24). Appellant has indicated that claim 22 should be allowed because it further limits claim 19, however appellant has not provided further arguments for this statement. As such, examiner recites the same reasoning used in the Office Action for the rejection of claim 22.

(28) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that for claim 23 in view of the arguments set forth above, it is respectfully submitted that "a means for establishing a session with a management server associated with an application on behalf of a remote client, wherein establishing the session with the management

server further comprises authenticating means for authenticating the unified session manager to the management server, wherein the authenticating means is virtually transparent to the client" is neither disclosed nor suggested in Araujo.

In response to argument (28), examiner asserts that Araujo does at least suggest this feature. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN. Thus as recited in the Office Action, since the connection utilizes SSL, it is seen that it would be obvious for the components to perform authentication.

(29) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that for claim 24 in view of the arguments set forth above, it is respectfully submitted that "an establisher configured to establish a session with a management server associated with an application on behalf of a remote client, wherein the session is established with the management server by an authentication with a unified session manager to the management server, and wherein the authentication is virtually transparent to the remote client" is neither disclosed nor suggested in Araujo.

In response to argument (29), examiner asserts that Araujo does at least suggest this feature. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN. Thus as recited in the Office Action, since the connection utilizes SSL, it is seen that it would be obvious for the components to perform authentication.

(30) Regarding the rejection of claims 1, 2, 4-9, 11-16 and 18-25 under 35 U.S.C. 103(a) as being unpatentable over US Pub. No. 2001/0047406 to Araujo et al. (hereinafter "Araujo"), appellant argues that for claim 25 in view of the arguments set forth above, it is respectfully submitted that "establishing a session between a unified session manager and a management server associated with the application, wherein establishing the session with the management server further comprises authenticating the unified session manager to the management server, wherein the authentication is virtually transparent to the client device" is neither disclosed nor suggested in Araujo.

In response to argument (30), examiner asserts that Araujo does at least suggest this feature. Paragraph [0109] of Araujo states that for the Netilla Virtual Office, all information transfer is protected by SSL. Then paragraph [0110] of Araujo discloses once virtual office

software (400) has appropriately processed the information by providing suitable protocol conversion (including performing SSL operations on the data), that information flows directly from software (400) to that office application accessible through the LAN via path (402). Accordingly the virtual office software is seen to perform SSL operations on the data that flows directly from itself to the office application accessible through the LAN. Thus as recited in the Office Action, since the connection utilizes SSL, it is seen that it would be obvious for the components to perform authentication.

(31) Regarding the rejection of claim 25 under 35 U.S.C. 101 as being non-statutory, appellant argues that the Office Action has not identified any place where the term "computer-readable medium" is defined in such a way as to include signals. Quite to the contrary, the specification provides at page 5, line 18, and following several examples of computer readable media without ever once identifying a signal as such a medium.

In response to argument (31), examiner asserts that the provided section does not support appellant's argument. Page 5, line 18 recites "LAN/WAN 104 is enabled to employ any form of computer readable media for communicating information from one electronic device to another". It does not appear that this is talking about the same computer readable medium being claimed. This portion discusses that the network is able to support any computer readable media for communicating information during the invention, not a computer readable medium embodying a computer program. In addition, should appellant feel the section still supports the invention being statutory, since LAN/WANs are communication networks and applicant's specification states these can include wireless links (Page 5 line 29) it would appear that this would support

examiners original interpretation. There does not appear to be any other portion in the specification that further discusses computer readable medium. Thus in view of a limiting definition of computer readable medium examiner has given the term computer readable medium its broadest reasonable interpretation. Such an interpretation includes both statutory interpretations such as various physical media, however it also includes non-statutory interpretations such as various propagation media. Accordingly it is seen that in view of no further description of computer readable medium, the term would include non-statutory embodiments.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Kevin S Mai/

Examiner, Art Unit 2456

Conferees:

/Kenny S Lin/

Primary Examiner, Art Unit 2452

/Bunjob Jaroenchonwanit/

Supervisory Patent Examiner, Art Unit 2456